

# Chaos-Based Image Encryption with Salp Swarm Key Optimization

Supriya Khaitana<sup>1</sup> | Shrddha Sagar<sup>2</sup> | Rashi Agarwal<sup>3</sup>

<sup>1,2</sup>School of Computing Science & Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India, Supriyakhaitan21@gmail.com

<sup>3</sup>Department of MCA, Galgotias College of Engineering & Technology, Greater Noida, Uttar Pradesh, India,

## To Cite this Article

Supriya Khaitana, Shrddha Sagar, Rashi Agarwal, "Chaos-based Image Encryption with Salp Swarm Key Optimization", *International Journal of Engineering Technology and Basic Sciences*, Vol. 01, Issue 01, August 2021, pp.-011-018.

## ABSTRACT

*Substantial data are being transmitted via the unsecured channel and the necessity to protect these data comes with this big transmission. Therefore, various encryption methods have been developed to achieve security during transmission. Chaos-based maps are extensively utilised for encryption of images because of their features such as their pseudo-random sensitivity. Inspired by researchers, we presented an image security technique based on a chaotic tent map, coupled with the Salp Swarm Algorithm (SSA). In each round, a diffusion and permutation are performed to secure it. To encrypt and decrypt data, a basic XOR algorithm is employed. Different statistical analyses of the pictures were done and the findings were analysed to support the efficiency of the approaches offered.*

**KEYWORDS:** Tent map, Salp Swarm Optimization, Encryption, Chaotic Map, Image Encryption

Copyright © 2021 International Journal of Engineering Technology and Basic Sciences  
All rights reserved.

## I. INTRODUCTION

The worldwide spread of the coronavirus pandemic has allowed the globe to look again at the fast expansion of digital communication technologies. The lock-down world has led to the popularisation of digital resources and information storage. Secure and decisive digital media monitoring is needed here. A large amount of information, including images, text, audio and video, is shared online. Image protection is being taken into account today, because photographs might include classified data and computerised image data has become commonplace. Imaging encryption often involves two stages: removal and highlight encryption [20-21]. Determination of features is one essential component of a consent framework for multi-instances; for example, picture sequencing[22]. In applications such as video

conferencing, therapeutic imagery, mechanical or military imaging[23], multimedia data protection has progressively become significant. Through preparing and organising communication with the rapid progress of the digital picture, data security problems have steadily grown opaque. Image encoding has become an important area of research. Many methods have been developed for the secure transfer of this data.

Traditional AES, DES, IDEA and RSA encryption techniques show various disadvantages and vulnerabilities in digital picture encryption and high computing power to big images. These methods have poor entropy values and heavily correlated data and are therefore inadequate for encryption of images[1-3]. In view of the picture characteristics, thus, improved approaches were developed for multiple image encryption utilising several types of technology, such as DNA

encoding[4-6], scaleable encoding[7] and quantum theory[8-10]. In the recent decade, academics have been keen to examine the chaos-based system. In 1989, Matthews initially suggested a chaotic cryptographic algorithm[11]. Chaos is a non-linear dynamic system that is sensitive to its initial condition. They feature qualities like as unpredictable behaviour, ergodicity, and pseudo-randomness; this makes them attractive among encryption methods researchers.

Chaotic systems have features which fulfil the diffusion and confusion requirements necessary for a successful cryptographic method. The appealing aspect of a chaos-based system is its strong impact on its underlying situation, control criteria and simple use, resulting in high encryption rates by offering features such as avalanche effect, confusion and diffusion. Many scholars have suggested many types of chaos-based systems such as Arnold map [12], Hennon map [13] and Logistic Map [14], Lorentz map [15], tent map [16,17], hyperchaotic map [18,19].

## **II. RELATED WORK**

The chaos-based system has an extreme ergodic characteristic. Some are non-assault resistant[24-25], some have restricted key space[26-27]. In 2019 Zhou, M. et al. [28] developed a Joseph Ring to dynamically destruct the correlation between the pixels and scrap the pixel using complicated nonlinear processes and bit rearrangement. Liu. et al. [29] used a parametrically varying one-dimensional chaotic pixel shuffling map. Zero means logistic mappings govern the map of chaos. The parallel technique and a random number generator were introduced at Cavusaglu, U. et al.[30] to minimise the time consumed by encryption and decryption. The approach is nine times quicker than other techniques based on chaos. In 2019 Abbasi, S.F. et al. [31] presented a system of encryption that turns a picture into a meaningful one. In order to apply the features of confusion and dispersion, an interim logistic map was used. Various contemporary cryptography components such as Gray Substitution box and XOR were utilised to create an intermediate picture. Then the transform wavelet technique is used to acquire the relevant picture. The method proved resistant to numerous assaults, however while transformation data is lost.

Abbasi, et al. [32] utilised a symmetric fractal image technique, then a picture module operation

was conducted in order to obtain the encrypted image. The system proved robust to various assaults. A 3D, coloured pictures, substitution, and permutation space-based encryption technique has been suggested on an image utilising a modular, chaotic 3-D map [33]. The first stage is to transform 2-D pictures into 3-D images. The RGB spectrum was split into  $k$  equivalent portions in the second stage. Then XOR was used to alter the contents of each pixel or pixel group. Wu. et al.[34] used for encryption a highly complicated two-dimensional logistics map and conducted two-dimensional logistical permutation, diffusion and transposition. Each intermediary chip was a chip picture itself. The method presented was robust to cryptanalytic statistical and differential assaults.

Most academics have been working on symmetrical system-based key systems,[35] proposed an asymmetric system of encryption based on discrete mapping. The initial number of iterations and Hash function is used as the key, and the data is decrypted using a linear chaotic map. [36] presented a compressed sensing asymmetrical cylindrical diffraction encryption method to counter the phase recovery attack and information leakage. [37] Suggest an approach based on the chaotic four-wing system, which utilised a 512-bit hash function to build a one-time key to encrypt odd and even component RGB components.

In this work we integrated bio-inspired approaches of swarm optimization with the theory of chaos. The combination of these two has been utilised in numerous applications, although its use in cryptography is restricted. A two-step pixel confusion and diffusion technique is employed. For encryption employ chaos-based tent maps, and the Salp swarm method is used to optimise the decryption key. The paper is arranged accordingly: Sections 1 and 2 show the literature survey of the suggested approach and related works. Section 3 outlines the suggested approach, and Section 4 gives the results of the techniques presented, followed by the conclusions of the study.

## **III. PROPOSED METHODOLOGY**

The following components comprise a contemporary crypto-system, key generation algorithm, encryption and decryption algorithm.

Chaos key with the Tent Map: This study proposes a two-step procedure for generating the key. The key is 16 characters in length. This key is used to construct a key matrix sequence, similar to

the total pixels of an encrypted picture. Two keys are produced in the suggested asymmetric cryptography strategy, with the secret key using the chaotic tent map and with the public key using the optimization of the salp swarm, Figure 1 briefly describes the methodology presented.

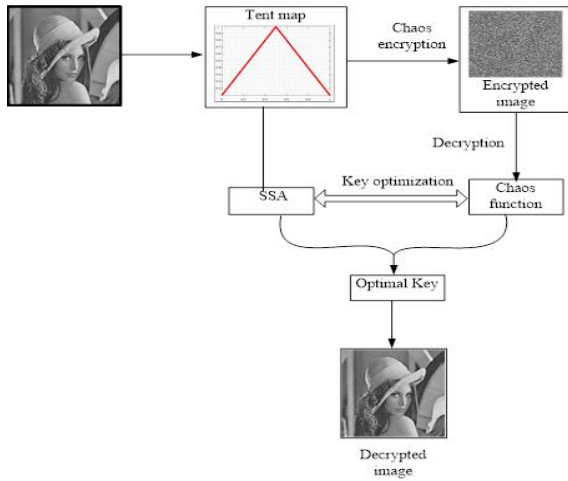


Figure 1. An overall diagram of the proposed method

The simple chaotic tent map is an iterated function between the interval of  $[0,1]$ . The name comes from the tent-like shape of the map, a discrete dynamic system given by the following equation:

$$v_{(i+1)} = f(v_i, \lambda) \quad (1)$$

$$f(v_i, \lambda) = \begin{cases} f_L(v_i, \lambda) = \lambda v_i, & \text{if } x_i < 0.5 \\ f_R(v_i, \lambda) = \lambda(1 - v_i) & \text{otherwise;} \end{cases} \quad (2)$$

Here,  $v_i \in [0,1]$ ,  $i \geq 0$ ,  $v_0$  is the system's starting value,  $\{v_0, v_1, \dots, v_n\}$  is the system's orbit. The map contains the control parameter  $\lambda$ , where  $\lambda \in [0,2]$ , depending on the control parameter  $\lambda$ . The map ranges from predictable to chaotic when  $\lambda = 1.99999$ ,  $x_0 = 0.000001$ , and  $i = 1$  to 200000. Fig. 2 shows the basic chaos function of the proposed technique. The key generation makes highly random key sequences using the chaotic method. The benefit of using a Tent map compared to another chaotic map is that it significantly simplifies the calculation; the higher-order iterates of the tent map involved in analyzing asymptotic dynamics are simple to measure.

Salp Swarm Optimization Algorithm: Salp swarm optimization was proposed by [38], a bio-inspired algorithm that imitates the behaviour of salp swarms and the social interaction of their populations. It is

a kind of salpiadae which has a translucent barrel-shaped body and tissues such as the structure of jellyfish. They dwell in the deep ocean and obtain nourishment using water forces to organise themselves as Salp chains. The Salp chains are divided into the leader and follower Salp in two sections. For a distinct variable, a d-dimensional search space defines the positions of Salp. The swarm's goal is food source  $f$ . The following algorithm is utilised in the approach given.

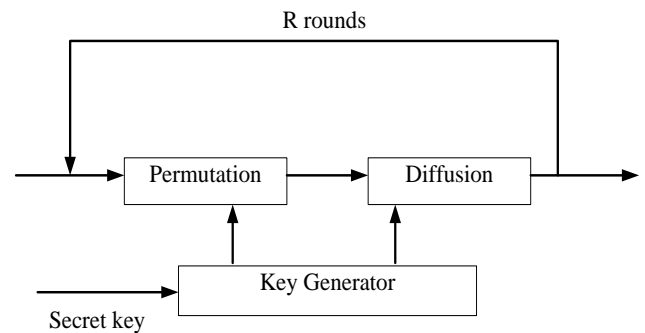


Figure 2. Basic Chaos function

Input: Salps, Number of iterations(T)

Output: Optimum Salp Position, Best Fitness Salp

Algorithm:

Generate Initial population of Salps  $x_i$ , where  $i = 1, 2, 3, \dots, n$  using chaotic tent map while (key! = optimized or  $t < \text{Maximum number of iterations}$ )

calculate the fitness of each Salp using the following equation

$$f = \min[\text{MSE}, \text{MAE}] \quad (3)$$

Set best Salp as  $b_x$

update position of  $e_1$

$$e_1 = 2e^{-\frac{4t}{T}} \quad (4)$$

where  $t = \text{current iteration}$  and  $T = \text{total number of iterations}$

for each  $x_i$

if ( $i < N/2$ )

update the position of leading salp

$$b_x = \begin{cases} f_x + e_1((u_x - l_x) * e_2 + l_x)e_3 \leq 0 \\ f_x - e_1((u_x - l_x) * e_2 + l_x)e_3 \leq 0 \end{cases} \quad (5)$$

Where  $e_2$  and  $e_3$  are random numbers between  $[0,1]$ ,  $u$  is upper bound,  $l$  is lower bound

else

update the position of follower salp

$$b_x = \frac{1}{2}gt^2 + v_0t \quad (6)$$

$$g = \frac{v_{\text{final}}}{v_0} \quad (7)$$

$$v = \frac{b - b_0}{t} \quad (8)$$



```

end if
end loop
update the position of Salp based on u and l
end while
return bx(optimal key)

```

**Encryption Phase:** This portion simply explains the simple image encryption algorithm based the chaotic key generated in the above step.

Input: Chaotic Key Sequence (P), Plain Image

Output: Encrypted Image

Algorithm:

Convert the key sequence into 8-bit blocks

Convert Plain Image into 8-bit blocks

for all blocks of size 8-bit

Key sequence 8-bit Image block

end loop

**Decryption Phase:** This section explains decryption by applying a simple XOR operation on the encrypted image and optimized key.

Input: Optimal Key Sequence, Encrypted Image

Output: Decrypted Image

Algorithm:

Convert the optimal key sequence into 8-bit blocks

Convert Cipher Image into 8-bit blocks

for all blocks of size 8-bit

Optimal Key sequence, 8-bit Encrypted Image-block

end loop

#### IV. EXPERIMENTAL RESULTS

For implementing the proposed technique, we have used MTLAB 7.12. The experiment is done on the Windows-10 Operating system with an Intel Core i5 processor with 4GB RAM and a 1.6GHz speed. All the images used are "512×512" sized that are freely available online. Some of the images used are shown in Figure 3.


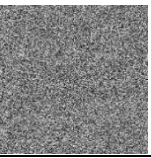
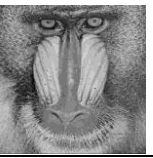
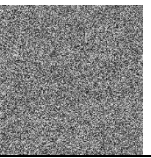

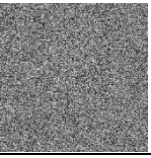

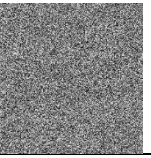

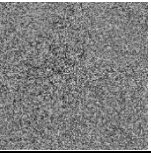

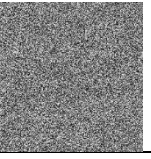
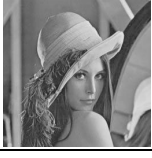
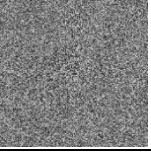
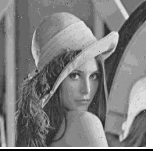
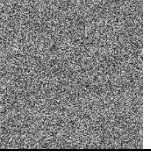

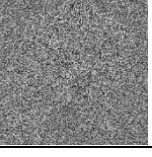

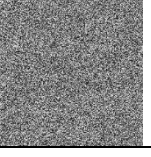


Figure 3. Sample input database images

**Evaluation Matrices:** To evaluate the performance of system some commonly used performance parameters like Encryption time, Entropy,

Cross-correlation, Unified Averaged Changed Intensity (UACI), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Decryption time are used.

Table 1. Image Sequence Encryption and Decryption

Input Image	Encrypted Image	Decrypted Image	Decrypted Image Different key
			
			
			
			
			

**Encryption Time & Decryption Time:** Encryption time is defined as amount of time it takes to convert plain image to cipher image. The amount of time machine takes to convert it back to plain image is known as decryption time. Table 2 shows the encryption and decryption time on some of the images.

Table 2. Time Analysis

	Encryption Time	Decryption Time
Lena	0.12	0.33
Baboon	0.12	0.2
Camera man	0.17	0.56

Barbara	0.13	0.2
Puppy	0.13	0.3

Entropy: Entropy is used to calculate the average unpredictability of data source and is given by

$$\text{Entropy} = - \sum_{x=0}^{G^L-1} \sum_{y=0}^{G^L-1} p(x,y) \times \log(p(x,y)) \quad (9)$$

Where p is the probability of occurrence of a symbol

Peak Signal to Noise Ratio (PSNR): The PSNR is a ratio of max power of a signal and the de-noised signal.

$$\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{\text{MSE}} \right) \quad (10)$$

Mean Square Error (MSE): The cumulative squared error between the signal's maximum power and its corrupting noise is known, and the mean square error.

$$\text{MSE} = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N [O(i,j) - O'(i,j)]^2 \quad (11)$$

Where;  $O(x,y)$  → Input image;  $O'(x,y)$  → De-noised image.

Table 3. Entropy, PSNR and MSE Analysis

	Entro py	PSNR	MSE
Lena	7.25	33.29	0.00046 8
Baboon	7.20	32.31	0.00058 7
Camera Man	7.079	32.01	0.00062 8
Barbara	7.53	32.47	0.00056 6
Puppy	7.46	31.957	0.00063 7

The Entropy, PSNR and MSE analysis of is shown in Table 3. All Entropy values are above 7 that is very close to the ideal entropy value 8 of  $256 \times 256$  Image. Closer is the entropy to its ideal value greater is the complexity of a cipher-image.

Differential cryptanalysis Attack (UACI& NPCR): The difference in the average intensity of pixels between the two images is measured by Unified Averaged Changed Intensity (UACI)

$$\text{UACI} = \frac{1}{L \times M} \left[ \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{N-1} \right] \times 100\% \quad (12)$$

NPCR gives the change rate of the pixels values in an image. If the value is nearing 100 presents, the system is highly sturdy against differential cryptanalysis attack.

$$\text{NPCR} = \frac{1}{L \times M} \sum_{i=1}^L \sum_{j=1}^M x(i,j) \times 100 \quad (13)$$

Where L and M are the width and height of an image, e1 and e2 represent cipher images after a 1-pixel value change.

Table 4. Differential Cryptoanalysis

	NPCR	UACI
Lena	99.50	33.46
Baboon	99.52	33.35
Camera Man	99.60	33.34
Barbara	99.61	33.46
Puppy	99.60	33.43

For any algorithm to be secured from a differential cryptanalysis attack, the value of NPCR needs to be above 99, and UACI needs to be above 33. both NPCR and UACI in table 4 shows the proposed scheme is resistant to differential cryptanalysis attack.

Cross-Correlation: The cross-connection is a proportion of closeness of two arrangements as an element of the relocation of one comparative with the other. For any two vectors, X and Y cross-correlation is given by eq. 12.

$$\begin{aligned} E(x) &= \frac{1}{N} \sum_{i=1}^N x_i \\ D(x) &= \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \\ \text{cov}(x,y) &= \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(x))^2 \\ r_{xy} &= \frac{\text{cov}(x,y)}{\sqrt{D(x)D(y)}} \end{aligned} \quad (14)$$

Where E is expected value and x and y are pixel coordinates. The pixels of plain image are highly correlated to each other. A good encryption algorithm breaks the linearity of this relation it can be seen from Table 5 original image has correlation of more than 0.99 which has been decreased by the proposed technique.

Table 5. Correlation Analysis

	Correlat ion	Correlation Analysis Encrypted Image		
		Horizon tal	Vertical	Diagona l
Lena	0.9917	0.0061 1	-0.028 20	0.0058 3
Baboon	0.9859	0.0061 7	0.0086 8	0.018 56

Camera Man	0.9946	0.0082	-0.024	0.0077
Barbara	0.9921	0.0076	0.0107	-0.006
Puppy	0.9936	0.0071	0.0110	0.0085
		9	46	9
		6	7	23
		1	5	6

Distribution is plotted to show the correlation between two adjacent pixels horizontally in an Input and Encrypted Leena Image; refer to Figure 5. With the plot, it can be seen the randomness of pixel relation in Encrypted image.

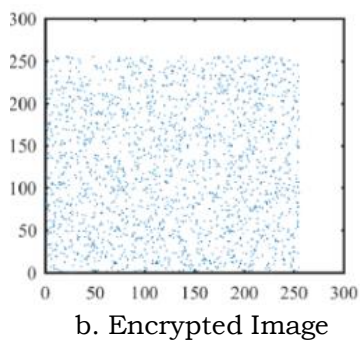
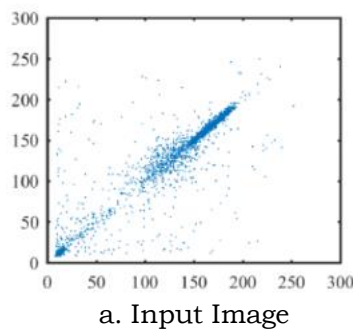
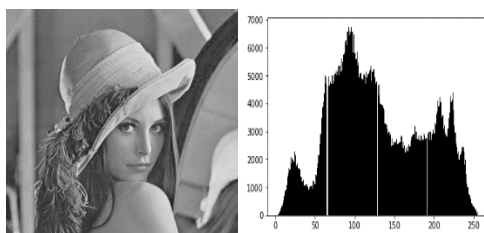
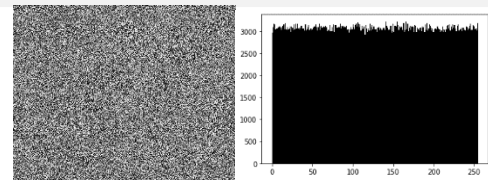


Figure4. Distribution of adjacent horizontal pixels of Input and Encrypted Lenna Image

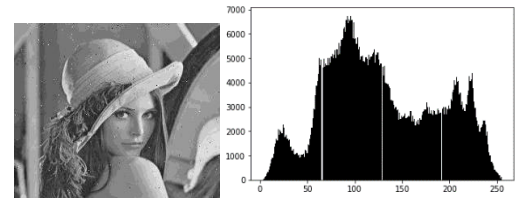
Histogram Analysis: Histogram characterizes the diffusion of pixels where each color intensity lies between 0 to 255. Any histogram that is uniformly distributed can prevent the statistical attack. Figure 4, shows the Encrypted Lenna image histogram is evenly distributed, so it is resistant to statistical attack.



(a) Input Image



(b) Encrypted Image



(c) Decrypted Image

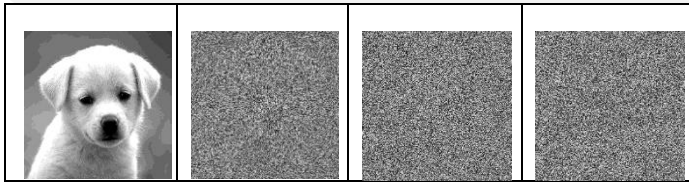
Figure 5. Histogram Analysis

Key Sensitivity Analysis: High key sensitivity is required in a cryptosystem; a minor change in the key leads to a significant output change. Table 4 shows an image encrypted with two keys with a one-bit difference, which leads to a different cipher image with more than 90% difference.

Table 6. Key Sensitivity Analysis

Input Image	Encrypt ed Image With Key 1	Encrypt ed Image With Key 2	Similarit y between both Images





## V. CONCLUSION

This study proposes a bio-inspired public key cryptosystem using chaotic tent map function to encrypt and optimise swarming in order to optimise decryption key. The picture and key are split in 8-bit blocks and a basic XOR operation has been performed. The suggested methodological performance such as crypt time, entropy, cross-relation, UACI, PSNR, MSE, MAE is analysed using different performance measures. The average entropy estimated at 7.30 may be demonstrated by the key sensitivity analysis as the change in an image results in a change of more than 90 percent. The outcome is a better system of chaotic public key than the existing standard approaches. An evolutionary algorithm can be employed in future to provide potential to the cryptography process.

## REFERENCES

- [1] D. Chaotopadhyaya and M.K Mandal "Symmetric Key Chaotic Image Encryption Using Circle Map" International Journal of Science and Technology 4(5), 2012, pp-791-795.
- [2] R. Choudhary and Jb. Article "Multimedia Content Security using Image Encryption" International Journal of Computer Applications 7, 2014 pp-30-33.
- [3] N. K Pareek and V. Patidhar "Substitution-diffusion based Image Cipher "International Journal of Network Security & Its Applications 3(2), March 2011, pp-255-259.
- [4] Zhen, P., Zhao, G., Min, L., Jin, X.: Chaos-based image encryption scheme combining dna coding and entropy. Multimed. Tools Appl. 75(11), 6303–6319 (2016).
- [5] Lilian Huang , Shiming Wang , Jianhong Xiang , and Yi Sun, "Chaotic Color Image Encryption Scheme Using Deoxyribonucleic Acid (DNA) Coding Calculations and Arithmetic over the Galois Field ", Mathematical Problems in Engineering Volume 2020, Article ID 3965281, 22 pages.
- [6] Yuqiang Dou, Xiumin Liu, Haiju Fan, Ming Li, Cryptanalysis of a DNA and chaos based image encryption algorithm, Optik, Volume 145, 2017, Pages 456-464
- [7] Zhang, X., Feng, G., Ren, Y., Qian, Z.: Scalable coding of encrypted images. IEEE Trans. Image Process. 21(6), 3108–3114 (2012)
- [8] Yu-Guang Yang, J., Tian, H.L., Zhou, Y.-H., Shi, W.-M.: Novel quantum image encryption using one-dimensional quantum cellular automata. Inf. Sci. 345, 257–270 (2016)
- [9] Yang, Y.-G., Xia, J., Jia, X., Zhang, H.: Novel image encryption decryption based on quantum Fourier transform and double phase encoding. Quant. Inf. Process. 12(11), 3477–3493 (2013)
- [10] Zhou, R.-G., Qian, W., Zhang, M.-Q., Shen, C.-Y.: Quantum image encryption and decryption algorithms based on quantum image geometric transformations. Int. J. Theor. Phys. 52(6), 1802–1817 (2013).
- [11] Matthews, R.A.J. On the Derivation of a "Chaotic" Encryption Algorithm. Cryptologia, 13, 1989 29-42.
- [12] Mansouri, A., Wang, X. Image encryption using shuffled Arnold map and multiple values manipulations. Vis Comput (2020). <https://doi.org/10.1007/s00371-020-01791-y>
- [13] Mishra, Kapil & Saharan, Ravi. (2019). A Fast Image Encryption Technique Using Henon Chaotic Map: Proceedings of ICACIE 2017, Volume 1. 10.1007/978-981-13-1708-8\_30.
- [14] Pan, H., Lei, Y. & Jian, C. Research on digital image encryption algorithm based on double logistic chaotic map, Journal of Image Video Proc. 2018, 142 2018.
- [15] Al-hazaimah, Obaida & Al-Jamal, Mohammad & Alhindawi, Nounh & Omari, Abedalkareem. (2019). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. Neural Computing and Applications. 31. 1-11. 10.1007/s00521-017-3195-1.
- [16] Li, C., Luo, G., Qin, K. et al. An image encryption scheme based on chaotic tent map. Nonlinear Dynamics 87, 2017, pp no. 127–133.
- [17] A., Mohammed & Faragallah, Osama., Efficient Chaotic Tent Map-based Image Cryptosystem. International Journal of Computer Applications. 167, 12-17, 2017.
- [18] Chen, C. ,Sun H.K. and S. B. He, "A class of higher-dimensional hyperchaotic maps," Eur. Phys. J. Plus, 134, 410, 2019.
- [19] Y. Li, W. K. S. Tang, and G. Chen, "Generating hyperchaos via state feedback control," International Journal of Bifurcation and Chaos, 15(10), 2005, pp. 3367–3375.
- [20] X. Wang, H. Zhao, L. Feng, X. Ye and H. Zhang, " High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices." Optics and Lasers in Engineering, Vol. 122, pp. 225–238, 2019.
- [21] P. V. Ramaraju, G. N. Raju and P. R. Krishna, "Image encryption after hiding (IEAH) technique for color images," International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016, pp. 1202-1207
- [22] S. Khaitan, R. Agarwal and M. Kaur, "Novel Method of Secure Communication using Logistic Map" International Journal of Recent Technology and Engineering, Vol. 8, no. 2S7, pp. 603-607, 2019.

- [23] G. Ye and K. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map", *Nonlinear Dyn* Vol. 69, pp. 2079–2087, 2012.
- [24] G. Chen, Y. Mao, Chui CK "A symmetric image encryption scheme based on 3D chaotic cat maps", *Journal of Chaos Solitons and Fractals* Vol. 21, no. 3, pp. 749–761, 2004.
- [25] Y. Liu, J. Zhang and D. Han, "A multidimensional chaotic image encryption algorithm based on the region of interest" *Multimed Tools Appl* Vol. 79, P17669–17705, 2020.
- [26] C. Hongjun and W. Xingyuan "Color image encryption using spatial bit-level permutation and high-dimension chaotic system", *OptCommun* Vol. 284, no16-17, pp. 3895–3903, 2011.
- [27] Yaobinmao, Guanrongchen and Shiguolian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", *International Journal of Bifurcation and Chaos*, Vol. 14, no. 10, pp. 3613-3624, 2004.
- [28] Zhou, Mengran & Xin, M.. (2019). Image Encryption Algorithms Based on Chaos Through Dual Scrambling of Dynamic Josephus Ring and Bit: Applications and Techniques in Cyber Security and Intelligence. 10.1007/978-3-319-98776-7\_16.
- [29] Liu, Lingfeng & Miao, Suoxia. (2016). A new image encryption algorithm based on logistic chaotic map with varying parameter. SpringerPlus. 5. 10.1186/s40064-016-1959-1.
- [30] Cavusogul, U., Kacar, S. "A Novel Parallel Image Encryption Algorithm based on chaos." *Cluster Computing*, 2019, Volume 22, Number 4, Page 1211
- [31] Abbasi, Saadullah & Ahmad, Jawad & Khan, Jan Sher & Khan, Muazzam & Sheikh, Shehzad. (2019). Visual Meaningful Encryption Scheme Using Intertwining Logistic Map: Proceedings of the 2018 Computing Conference, Volume 2. 10.1007/978-3-030-01177-2\_56..
- [32] Rozouvan, V. "Modulo image encryption with fractal keys." *Optics and Lasers in Engineering* Volume 47, Issue 1, January 2009, Pages 1-6
- [33] Broumandnia, A. "The 3D modular chaotic map to digital color image encryption" *Future Generation Computer Systems* Volume 99, October 2019, Pages 489-499.
- [34] Wu, Y., Noonan, J.P., Yang, G. and Jin, H. "Image Encryption using two dimensional logistic map " *Journal of Electronic Imaging*." 21. 3014-. 10.1117/1.JEI.21.1.013014.
- [35] Dong, C. Asymmetric color image encryption scheme using discrete-time map and hash value. *Optik* 126, 2571–2575. <https://doi.org/10.1016/j.matcom.2020.05.0168> (2015).
- [36] Wu, C., Wang, Y., Chen, Y., Wang, J. & Wang, Q. Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain. *Opt. Commun.* 431, 203–209. <https://doi.org/10.1016/j.optcom.2018.09.034> (2019).
- [37] Liu, H., Kadir, A. & Li, Y. Asymmetric color pathological image encryption scheme based on complex hyper chaotic system. *Optik* 127, 5812–5819 (2016).
- [38] SeyedaliMirjalili, Amir H. Gandomi, Seyedeh Zahra Mirjalili, ShahrzadSaremi, Hossam Faris, Seyed Mohammad Mirjalili, Salp Swarm Algorithm: A bio-inspired optimizer for engineering design problems, *Advances in Engineering Software*, Volume 114, pp no. 163-191, 2017